## AMENDMENTS TO CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

**Listing of Claims:**

1. (Currently Amended) A method for protecting a secured data storage (1), by using sensors (2) to detect an external action on a component, said component containing the secured data storage (1) and an overwritable memory, said method comprising the steps of:

determining that an attack has occurred based on undershooting or overshooting of a threshold on one of the sensors (2);

at least partially erasing a content of the secured data storage (1) upon determining that an attack has occurred;

permanently monitoring a status of the sensors (2); and

recording status data of the sensors (2) by storing the status data cyclically in ~~an~~ said overwritable memory (3).

2. (Canceled)

3. (Previously Presented) A method according to claim 1, wherein the step of recording said status data comprises the step of storing the status data of the sensors (2) in a nonvolatile memory (4).

4. (Previously Presented) A method according to claim 1, wherein the step of recording said status data comprises the step of storing the status data of the sensors (2) in a volatile temporary memory (3) and when an attack is signaled, transferring the status data contained in the temporary memory (3) to a nonvolatile final memory (4).

5. (Previously Presented) A method according to claim 4, wherein when an attack is signaled at least the status data of the sensor signaling the attack are stored directly in the final memory (4).

6. (Previously Presented) A method according to claim 5, wherein the status data are stored in the temporary memory (3) in digitally coded form, and direct storage of the status data in the final memory (4) is done in analog form when an attack is signaled.

7. (Previously Presented) A method according to claim 1, further comprising the step of, if the supply voltage (*VCC*) fails, maintaining a power supply to the sensors (2) and/or the secured data storage (1), and/or further components (3, 4, 5, 6, 7) required for carrying out the method with a battery for a certain time period.

8. (Previously Presented) A method according to claim 5, wherein after an attack is signaled the content of the secured data storage (1) is first erased, then the current status data at least of the sensor signaling the attack are stored in the final memory (4), and subsequently the status data contained in the temporary memory (3) are transferred to the final memory (4).

9. (Previously Presented) A method according to claim 1, wherein the step of recording said status data comprises the step of transferring the status data stored in the temporary memory (3) to the final memory (4) in reverse chronological order in terms of their age, the status data of the sensor signaling the attack being transferred first and then the status data of the other sensors.

10. (Currently Amended) A security processor, comprising:

a secured data storage (1);

an overwritable memory;

sensors (2) for detecting external action on the security processor and/or the secured data storage (1);

a sensor evaluation device (5) which at least partly erases a content of the secured data storage (1) when a threshold is overshot on one of the sensors (2); and

a data recording device (6) which permanently records the status data of the sensors (2) in ~~an~~ said overwritable memory (3) in which the status data of the sensors (2) is cyclically stored by the data recording device (6).

11. (Canceled)

12. (Previously Presented) A security processor according to claim 10, wherein said memory includes a volatile temporary memory (3) in which the status data of the sensors (2) are stored permanently, and a nonvolatile final memory (4) to which the status data contained in the temporary memory (3) are transferred when an attack is signaled.

13. (Previously Presented) A security processor according to claim 10, wherein said memory includes a volatile temporary memory (3) in which the status data of the sensors (2) are stored permanently, and a nonvolatile final memory (4) to which the status data contained in the temporary memory (3) are transferred when an attack is signaled.

14. (Previously Presented) A security processor according to claim 14, further comprising an analog-to-digital converter (7) which digitally codes the analog status data before storage.

15. (Previously Presented) A security processor according to claim 13, wherein the sensor evaluation device (5) is connected with the final memory (4) and when an attack is signaled at least the status data of the sensor signaling the attack are stored directly in the final memory (4).

16. (Previously Presented) A security processor according to claim 1, further comprising a battery which maintains a power supply to the sensors (2), and/or secured data storage (1), and/or sensor evaluation device (5), and/or data recording device (6), and/or data recording device (6) for the status data of the sensors for a certain time period if the supply voltage (*VCC*) fails.

17-18. (Canceled)